

POTTER HANDY LLP

Mark D. Potter (SBN 166317)

mark@potterhandy.com

James M. Treglio (SBN 228077)

jimt@potterhandy.com

100 Pine St., Ste 1250

San Francisco, CA 94111

Tel: (858) 375-7385

Fax: (888) 422-5191

Attorneys for Plaintiff

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

STEPHEN BURTON, on behalf of
himself and all others similarly situated,

Plaintiff,

vs.

LINCARE INC., a Delaware corporation;
and DOES 1 through 100, inclusive,

Defendants.

) Case No. 5:22-cv-04763-EJD

) Honorable Edward J. Davila

) **CLASS ACTION**

) **FIRST AMENDED CLASS
COMPLAINT FOR DAMAGES
AND INJUNCTIVE RELIEF (FOR
VIOLATIONS OF:**

) **(1) THE CONFIDENTIALITY
OF MEDICAL
INFORMATION ACT, CIVIL
CODE §§ 56, *ET SEQ.*);**

) **(2) CALIFORNIA UNFAIR
COMPETITION LAW, Cal.
Bus. & Prof. Code §17200, *et
seq.*;**

) **(3) CALIFORNIA CONSUMER
RECORDS ACT, Cal. Civ.
Code § 1798.82, *et seq.***

DEMAND FOR JURY TRIAL

1 Class Representative Stephen Burton (“Class Representative” or “Plaintiff”),
 2 by and through his attorneys, individually and on behalf of others similarly situated,
 3 alleges upon information and belief as follows:

4 **I.**

5 **INTRODUCTION**

6 1. Under the Confidentiality of Medical Information Act, Civil Code §§ 56,
 7 *et seq.* (hereinafter referred to as the “Act”), Plaintiff and all other persons similarly
 8 situated, had a right to keep their personal medical information provided to
 9 Defendants Lincare Inc. (“Lincare,” “Defendant,” or “Defendants”) confidential.
 10 The short title of the Act states, “The Legislature hereby finds and declares that
 11 persons receiving health care services have a right to expect that the confidentiality
 12 of individual identifiable medical information derived by health service providers be
 13 reasonably preserved. It is the intention of the Legislature in enacting this act, to
 14 provide for the confidentiality of individually identifiable medical information,
 15 while permitting certain reasonable and limited uses of that information.” The Act
 16 specifically provides that “a provider of health care, health care service plan, or
 17 contractor shall not disclose medical information regarding a patient of the provider
 18 of health care or an enrollee or subscriber of a health care service plan without first
 19 obtaining an authorization...” Civil Code. § 56.10(a). The Act further provides that
 20 “Every provider of health care, health care service plan, pharmaceutical company,
 21 or contractor who creates, maintains, preserves, stores, abandons, destroys, or
 22 disposes of medical records shall do so in a manner that preserves the confidentiality
 23 of the information contained therein. Any provider of health care, health care service
 24 plan, pharmaceutical company, or contractor who negligently creates, maintains,
 25 preserves, stores, abandons, destroys, or disposes of medical records shall be subject
 26 to the remedies ... provided under subdivisions (b) ... of Section 56.36.” Civil Code
 27 § 56.101(a).
 28

1 2. Civil Code § 56.36(b) provides Plaintiff, and all other persons similarly
2 situated, with a private right to bring an action against Defendant for violation of Civil
3 Code § 56.101 by specifically providing that “[i]n addition to any other remedies
4 available at law, any individual may bring an action against any person or entity who
5 has negligently released confidential information or records concerning him or her in
6 violation of this part, for either or both of the following: (1) ... nominal damages of
7 one thousand dollars (\$1,000). In order to recover under this paragraph, *it shall not*
8 *be necessary that the plaintiff suffered or was threatened with actual damages.* (2)
9 The amount of actual damages, if any, sustained by the patient.” (Emphasis added.)

10 3. This class action is brought on behalf of Plaintiff and a putative class
11 defined as all citizens of the State of California who were patients of Lincare Inc. on
12 or before September 10, 2021, and who received notices from Lincare that their
13 information was compromised (“Breach Victims,” the “Class,” or the “Class
14 Members”).

15 4. As alleged more fully below, Defendant created, maintained, preserved,
16 and stored Plaintiff and the Class members’ personal medical information onto the
17 Defendant’s computer network prior to September 10, 2021. Due to Defendant’s
18 mishandling of personal medical information recorded onto the Defendant’s computer
19 network, there was an unauthorized release of Plaintiff and the Class members’
20 confidential medical information that occurred between September 10, 2021 and
21 September 29, 2021, in violation of Civil Code § 56.101 of the Act.

22 5. As alleged more fully below, Defendant negligently created, maintained,
23 preserved, and stored Plaintiff and the Class members’ confidential medical
24 information in a non-encrypted format onto a data server which became accessible to
25 an unauthorized person, without Plaintiff and the Class members’ prior written
26 authorization. This act of providing unauthorized access to Plaintiff and the Class
27 Members’ confidential medical information onto the internet continuously constitutes
28 an unauthorized release of confidential medical information in violation of Civil Code

1 § 56.101 of the Act. Because Civil Code § 56.101 allows for the remedies and
2 penalties provided under Civil Code § 56.36(b), Class Representative, individually
3 and on behalf of others similarly situated, seeks nominal damages of one thousand
4 dollars (\$1,000) for each violation under Civil Code § 56.36(b)(1). Additionally,
5 Class Representative, individually and on behalf of others similarly situated, seeks
6 injunctive relief for unlawful violations of Business and Professions Code §§ 17200,
7 *et seq.*

8 6. Class Representative does not seek any relief greater than or different
9 from the relief sought for the Class of which Plaintiff is member. The action, if
10 successful, will enforce an important right affecting the public interest and would
11 confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of
12 persons. Private enforcement is necessary and places a disproportionate financial
13 burden on Class Representative's stake in the matter.

14 II.

15 **JURISDICTION AND VENUE**

16 7. This Court has jurisdiction over this action pursuant to the Class Action
17 Fairness Act of 2005 (CAFA), 28 U.S.C. § 1332(d), in that according to Defendants'
18 Notice of Removal (1) the Class as defined above has 100 or more members; (2) the
19 aggregate claim exceeds \$5 million, exclusive of interest and costs; and (3) Plaintiff
20 and the Class are citizens of the State of California, and Defendants are citizens of the
21 State of Florida and/or Delaware.

22 8. At all relevant times, Plaintiff and the Class Members are citizens of the
23 State of California who utilized Defendants' services in California. At all relevant
24 times, Plaintiff and the Class Members utilized Defendants' services for respiratory
25 care, INR testing, enteral services, among others.

26 9. The Court also has personal jurisdiction over the parties because Plaintiff
27 and the Defendants have submitted to the jurisdiction of the Court and Defendants
28 have transacted business within this judicial district, in Santa Cruz County and in the

1 State of California; and the violations of law herein described have been committed
2 within this judicial district, in Santa Cruz County and in the State of California.
3 Moreover, by doing business in this judicial district and committing violations of the
4 California Civil Code and the California Business and Professions Code in this
5 judicial district, Defendants' conduct has had an adverse effect upon the finances of
6 residents of this judicial district.

7 **III.**

8 **PARTIES**

9 **A. PLAINTIFF**

10 10. Class Representative Stephen Burton is a resident of the State of
11 California. At all times relevant, Plaintiff was a patient of Defendants. The
12 information provided by Plaintiff to Defendants included Plaintiff's medical
13 information. Thus, Plaintiff was a patient, as defined by Civil Code § 56.05(k).
14 Plaintiff's individual identifiable medical information derived by Defendant in
15 electronic form was in possession of Defendant, including but not limited to Plaintiff's
16 medical history, mental or physical condition, or treatment, including diagnosis and
17 treatment dates. Such medical information included or contained an element of
18 personal identifying information sufficient to allow identification of the individual,
19 such as Plaintiff's name, date of birth, addresses, medical record number, insurance
20 provider, electronic mail address, telephone number, or social security number, or
21 other information that, alone or in combination with other publicly available
22 information, reveals Plaintiff's identity. Since Defendant obtained Plaintiff's
23 information, Plaintiff has received numerous solicitations by mail from third parties
24 at an address he only provided to Defendant.

25 11. PLAINTIFF received from Defendant a notification that his personal
26 medical information and his personal identifying information were disclosed when an
27 unauthorized person gained access to Defendant's servers.

28 //

B. DEFENDANT

12. Defendant Lincare Inc. is a leading provider of high-quality, at-home respiratory care, INR testing, enteral services, and home medical supplies throughout the country. It is a Delaware corporation with its principal place of business located at 19387 US Hwy 19 N, Clearwater, FL 33764. Defendant operates throughout the State of California including in Santa Cruz, California. At all times relevant, Defendant is a “provider of health care” as defined by Civil Code § 56.05(m). Prior to September 10, 2021, Defendant created, maintained, preserved, and stored Plaintiff and the Class members’ individually identifiable medical information onto Defendant’s computer network, including but not limited to Plaintiff and the Class members’ medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiff and the Class members’ names, dates of birth, addresses, medical record numbers, insurance providers, electronic mail addresses, telephone numbers, or social security numbers, or other information that, alone or in combination with other publicly available information, reveals Plaintiff and the Class members’ identities.

C. DOE DEFENDANTS

13. The true names and capacities, whether individual, corporate, associate, or otherwise, of Defendants sued herein as DOES 1 through 100, inclusive, are currently unknown to the Plaintiff, who therefore sues the Defendants by such fictitious names under the Code of Civil Procedure § 474. Each of the Defendants designated herein as a DOE is legally responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of court and/or amend this complaint to reflect the true names and capacities of the Defendants designated hereinafter as DOES 1 through 100 when such identities become known. Any reference made to a

1 named Defendant by specific name or otherwise, individually or plural, is also a
2 reference to the actions or inactions of DOES 1 through 100, inclusive.

3 **D. AGENCY/AIDING AND ABETTING**

4 14. At all times herein mentioned, Defendants, and each of them, were an
5 agent or joint venturer of each of the other Defendants, and in doing the acts alleged
6 herein, were acting with the course and scope of such agency. Each Defendant had
7 actual and/or constructive knowledge of the acts of each of the other Defendants, and
8 ratified, approved, joined in, acquiesced and/or authorized the wrongful acts of each
9 co-defendant, and/or retained the benefits of said wrongful acts.

10 15. Defendants, and each of them, aided and abetted, encouraged and
11 rendered substantial assistance to the other Defendants in breaching their obligations
12 to Plaintiff and the Class, as alleged herein. In taking action, as particularized herein,
13 to aid and abet and substantially assist the commissions of these wrongful acts and
14 other wrongdoings complained of, each of the Defendants acted with an awareness of
15 his/her/its primary wrongdoing and realized that his/her/its conduct would
16 substantially assist the accomplishment of the wrongful conduct, wrongful goals, and
17 wrongdoing.

18 **IV.**

19 **FACTUAL ALLEGATIONS**

20 **A. The Data Breach**

21 16. Defendant Lincare Inc. is a leading provider of high-quality, at-home
22 respiratory care, INR testing, enteral services, and home medical supplies throughout
23 the country. With data stored regarding its patients nationwide, Lincare collects a
24 significant amount of sensitive data from current and former patients, as delineated
25 above.

26 17. On or around June 21, 2022, Defendant issued a letter (the "Notice") to
27 individuals, including Plaintiff, providing, for the first time, a notice "of a security
28 incident that may have involved the disclosure of some of your personal information."

1 18. In the Notice, Defendant notified consumers that when it became aware
2 of the unusual activity on September 26, 2021, it “took immediate action...to secure
3 its network and launched an investigation, including working with outside
4 cybersecurity experts to determine the source of the activity and potential impact on
5 Lincare’s network.”

6 19. Almost nine months later or on June 21, 2022, Defendant sent the Notice
7 stating that “The investigation confirmed that certain systems may have first been
8 accessed on September 10, 2021. The unauthorized access was blocked by September
9 29, 2021...On April 20, 2022, it was confirmed that your information was
10 involved...” (the “Data Breach”).

11 20. The Notice went on to say that as a result of the review, it was determined
12 that some of Plaintiff and the Class Members’ information may have been involved.
13 Defendant confirmed that some of Plaintiff’s information were present in the files that
14 were illegally accessed from Defendant’s server. Defendant failed to state in its
15 Notice when it identified that Plaintiff’s information was included in the Data Breach.

16 21. Yet, despite knowing many patients were in danger, Defendant did
17 nothing to warn Breach Victims until almost nine months after it discovered the Data
18 Breach and more than nine months after the actual date of the Data Breach, an
19 unreasonable amount of time under any objective standard. During this time, cyber
20 criminals had free reign to surveil and defraud their unsuspecting victims. Defendant
21 apparently chose to complete its internal investigation and develop its excuses and
22 speaking points before giving class members the information they needed to protect
23 themselves against fraud and identity theft.

24 22. During its investigation, Defendant “determined that the following types
25 of information relating to you were involved in this this incident: name, medical
26 information, which may include information concerning medical treatments you
27 received such as provider name, dates of service, diagnosis/procedure, and/or account
28 or record numbers.”

1 23. This was a staggering coup for cyber criminals and a stunningly bad
2 showing for Defendant. It would be even worse if the Breach Victims are minors as
3 this data breach will likely affect them for their entire lives.

4 24. It is apparent from Defendant's Notice that the Personal and Medical
5 information contained within the server was not encrypted or was inadequately
6 protected.

7 25. In spite of the severity of the Data Breach, Defendant has done very little
8 to protect Breach Victims. In the Notice, Defendant states that it is notifying Breach
9 Victims and it encourages the Breach Victims to remain vigilant against incidents of
10 identity theft and fraud, and to review their account statements and explanation of
11 benefits forms, and to monitor their free credit reports for suspicious activity, and to
12 detect errors. In effect, shirking its responsibility for the harm it has caused and
13 putting it all on the Breach Victims.

14 26. Defendant failed to adequately safeguard Plaintiff and Class members'
15 Personal and Medical Information, allowing cyber criminals to access this wealth of
16 priceless information and use it for more than nine months before Defendant warned
17 the criminals' victims, the Breach Victims, to be on the lookout.

18 27. Defendant failed to spend sufficient resources on monitoring external
19 incoming emails and training its employees to identify email-born threats and defend
20 against them.

21 28. Defendant had obligations created by the Health Insurance Portability
22 and Accountability Act ("HIPAA"), the Confidentiality of Medical Information Act
23 ("CMIA"), reasonable industry standards, its own contracts with its patients and
24 employees, common law, and its representations to Plaintiff and Class members, to
25 keep their Personal and Medical Information confidential and to protect the
26 information from unauthorized access.

27 29. Plaintiff and Class members provided their Personal and Medical
28 Information to Defendant with the reasonable expectation and mutual understanding

1 that Defendant would comply with its obligations to keep such information
2 confidential and secure from unauthorized access.

3 30. Indeed, as discussed below, Defendant promised Plaintiff and Class
4 members that it would do just that.

5 **B. Defendant Expressly Promised to Protect Personal and Medical**
6 **Information**

7 31. Defendant provides all clients, including Plaintiff and Class members,
8 its Company Privacy Policy, which states that:

9 SECURITY OF YOUR INFORMATION
10

11 The security of your Personally Identifiable Information is very
12 important to us, and Company takes reasonable steps to protect the
13 information you provide us from loss, misuse, unauthorized access,
14 disclosure, alteration, or destruction. We follow generally accepted
15 industry standards to safeguard your information, however, no data or
16 email transmission is ever fully secure or error free. Therefore, please
take special care in deciding what information to send us. We have
reasonable safeguards in place to protect your information, and we have
taken the following security measures: ...¹

17 32. Notwithstanding the foregoing assurances and promises, Defendant
18 failed to protect the Personal and Medical Information of Plaintiff and other Class
19 members from cyber criminals using relatively unsophisticated means to dupe its
20 patients, as conceded in the Notice to the Breach Victims.

21 33. If Defendant truly understood the importance of safeguarding patients'
22 Personal and Medical Information, it would acknowledge its responsibility for the
23 harm it has caused, and would compensate class members, provide long-term
24 protection for Plaintiff and the Class, agree to Court-ordered and enforceable changes
25 to its cybersecurity policies and procedures, and adopt regular and intensive training
26 to ensure that a data breach like this never happens again.

27
28 ¹ Lincare, "Company Privacy Policy," <https://www.lincare.com/en/policies/privacy>, last visited on July 15, 2022.

34. Defendant's data security obligations were particularly important given the known substantial increase in data breaches, including the recent massive data breach involving Illuminate Education, Horizon Actuarial Services, Partnership HealthPlan of California, Bako Diagnostics, Rite Aid, Discovery Practice Management, Fairchild Medical Center, Scripps Health, HealthNet, LabCorp, Quest Diagnostics, and American Medical Collections Agency. And given the wide publicity given to these data breaches, there is no excuse for Defendant's failure to adequately protect Plaintiff and Class members' Personal and Medical Information.

35. That information, is now in the hands of cyber criminals who will use it if given the chance. Much of this information is unchangeable and loss of control of this information is remarkably dangerous to consumers.

C. Defendant had an Obligation to Protect Personal and Medical Information under Federal and State Law and the Applicable Standard of Care

36. Defendant is an entity covered by HIPAA (45 C.F.R. § 160.102). As such, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

37. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

38. HIPAA's Security Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is held or transferred in electronic form.

1 39. HIPAA requires Defendant to “comply with the applicable standards,
2 implementation specifications, and requirements” of HIPAA “with respect to
3 electronic protected health information.” 45 C.F.R. § 164.302.

4 40. “Electronic protected health information” is “individually identifiable
5 health information . . . that is (i) Transmitted by electronic media; maintained in
6 electronic media.” 45 C.F.R. § 160.103.

7 41. HIPAA’s Security Rule requires Defendant to do the following:

- 8 a. Ensure the confidentiality, integrity, and availability of all electronic
9 protected health information the covered entity or business associate
10 creates, receives, maintains, or transmits;
11 b. Protect against any reasonably anticipated threats or hazards to the
12 security or integrity of such information;
13 c. Protect against any reasonably anticipated uses or disclosures of such
14 information that are not permitted; and
15 d. Ensure compliance by its workforce.

16 42. HIPAA also required Defendant to “review and modify the security
17 measures implemented . . . as needed to continue provision of reasonable and
18 appropriate protection of electronic protected health information.” 45 C.F.R. §
19 164.306(e).

20 43. HIPAA also required Defendant to “[i]mplement technical policies and
21 procedures for electronic information systems that maintain electronic protected
22 health information to allow access only to those persons or software programs that
23 have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

24 44. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also
25 required Defendant to provide notice of the breach to each affected individual
26
27
28

1 “without unreasonable delay and *in no case later than 60 days following discovery*
2 *of the breach.*”²

3 45. Defendant was also prohibited by the Federal Trade Commission Act
4 (“FTC Act”) (15 U.S.C. §45) from engaging in “unfair or deceptive acts or practices
5 in or affecting commerce.” The Federal Trade Commission (“FTC”) has concluded
6 that a company’s failure to maintain reasonable and appropriate data security for
7 consumers’ sensitive personal information is an “unfair practice” in violation of the
8 FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

9 46. As described before, Defendant is also required (by the California
10 Consumer Records Act (“CCRA”), CMIA and various other states’ laws and
11 regulations) to protect Plaintiff and Class members’ Personal and Medical
12 Information, and further, to handle any breach of the same in accordance with
13 applicable breach notification statutes.

14 47. In addition to their obligations under federal and state laws, Defendant
15 owed a duty to Breach Victims whose Personal and Medical Information was
16 entrusted to Defendant to exercise reasonable care in obtaining, retaining, securing,
17 safeguarding, deleting, and protecting the Personal and Medical Information in its
18 possession from being compromised, lost, stolen, accessed, and misused by
19 unauthorized persons. Defendant owed a duty to Breach Victims to provide
20 reasonable security, including consistency with industry standards and requirements,
21 and to ensure that its computer systems and networks, and the personnel responsible
22 for them, adequately protected the Personal and Medical Information of the Breach
23 Victims.

24 48. Defendant owed a duty to Breach Victims whose Personal and Medical
25 Information was entrusted to Defendant to design, maintain, and test its computer
26

27 ² Breach Notification Rule, U.S. Dep’t of Health & Human Services, [https://www.hhs.gov/hipaa/for](https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html)
28 [professionals/breach-notification/index.html](https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html) (emphasis added).

1 systems and email system to ensure that the Personal and Medical Information in
2 Defendant's possession was adequately secured and protected.

3 49. Defendant owed a duty to Breach Victims whose Personal and Medical
4 Information was entrusted to Defendant to create and implement reasonable data
5 security practices and procedures to protect the Personal and Medical Information in
6 their possession, including adequately training its employees and others who accessed
7 Personal Information within its computer systems on how to adequately protect
8 Personal and Medical Information.

9 50. Defendant owed a duty to Breach Victims whose Personal and Medical
10 Information was entrusted to Defendant to implement processes that would detect a
11 breach on its data security systems in a timely manner.

12 51. Defendant owed a duty to Breach Victims whose Personal and Medical
13 Information was entrusted to Defendant to act upon data security warnings and alerts
14 in a timely fashion.

15 52. Defendant owed a duty to Breach Victims whose Personal and Medical
16 Information was entrusted to Defendant to adequately train and supervise its
17 employees to identify and avoid any phishing emails that make it past its email
18 filtering service.

19 53. Defendant owed a duty to Breach Victims whose Personal and Medical
20 Information was entrusted to Defendant to disclose if its computer systems and data
21 security practices were inadequate to safeguard individuals' Personal and Medical
22 Information from theft because such an inadequacy would be a material fact in the
23 decision to entrust Personal and Medical Information with Defendant.

24 54. Defendant owed a duty to Breach Victims whose Personal and Medical
25 Information was entrusted to Defendant to disclose in a timely and accurate manner
26 when data breaches occurred.

27 55. Defendant owed a duty of care to Breach Victims because they were
28 foreseeable and probable victims of any inadequate data security practices.

D. A Data Breach like Defendant's Results in Debilitating Losses to Consumers

56. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.³ Cyber criminals can leverage Plaintiff and Class members' Personal and Medical Information that was stolen in the Data Breach to commit thousands-indeed, millions-of additional crimes, including opening new financial accounts in Breach Victims' names, taking out loans in Breach Victims' names, using Breach Victims' names to obtain medical services and government benefits, using Breach Victims' Personal Information to file fraudulent tax returns, using Breach Victims' health insurance information to rack up massive medical debts in their names, using Breach Victims' health information to target them in other phishing and hacking intrusions based on their individual health needs, using Breach Victims' information to obtain government benefits, filing fraudulent tax returns using Breach Victims' information, obtaining driver's licenses in Breach Victims' names but with another person's photograph, and giving false information to police during an arrest. Even worse, Breach Victims could be arrested for crimes identity thieves have committed.

57. Personal and Medical Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.

58. This was a financially motivated data breach, as the only reason cyber criminals stole Plaintiff and the Class members' Personal and Medical Information from Defendant was to engage in the kinds of criminal activity described above, which will result, and has already begun to, in devastating financial and personal losses to Breach Victims.

³ "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

59. This is not just speculative. As the FTC has reported, if hackers get access to Personal and Medical Information, they **will** use it.⁴

60. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information **may continue for years**. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁵

61. For instance, with a stolen social security number, which is part of the Personal and Medical Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.⁶ Identity thieves can also use the information stolen from Breach Victims to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

62. Medical identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, “medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013,” which is more “than identity thefts involving banking and finance, the government and the military, or education.”⁷

63. “Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy Forum. “Victims often experience financial repercussions

⁴ Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM’N (May 24, 2017), <https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info>.

⁵ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, <https://www.gao.gov/assets/270/262904.html> (emphasis added).

⁶ See, e.g., Christine Di Gangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

⁷ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>.

1 and worse yet, they frequently discover erroneous information has been added to their
2 personal medical files due to the thief's activities."⁸

3 64. As indicated by Jim Trainor, second in command at the FBI's cyber
4 security division: "Medical records are a gold mine for criminals—they can access a
5 patient's name, DOB, Social Security and insurance numbers, and even financial
6 information all in one place. Credit cards can be, say, five dollars or more where PHI
7 can go from \$20 say up to—we've seen \$60 or \$70 [(referring to prices on dark web
8 marketplaces)]."⁹ A complete identity theft kit that includes health insurance
9 credentials may be worth up to \$1,000 on the black market.¹⁰

10 65. If, moreover, the cyber criminals also manage to steal financial
11 information, credit and debit cards, health insurance information, driver's licenses and
12 passports—as they did here—there is no limit to the amount of fraud that Defendant
13 has exposed the Breach Victims to.

14 66. A study by Experian found that the average total cost of medical identity
15 theft is "about \$20,000" per incident, and that a majority of victims of medical identity
16 theft were forced to pay out-of-pocket costs for healthcare they did not receive in
17 order to restore coverage.¹¹ Almost half of medical identity theft victims lose
18 their healthcare coverage as a result of the incident, while nearly one-third saw their
19 insurance premiums rise, and forty percent were never able to resolve their identity
20 theft at all.¹²

21 ⁸ *Id.*

22 ⁹ ID Experts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, New Ponemon Study
23 Shows, <https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat>

24 ¹⁰ *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The
25 Global State of Information Security Survey 2015, <https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>

26 ¹¹ See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010),
<https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>.

27 ¹² *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN,
28 <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>.

1 67. As described above, identity theft victims must spend countless hours
2 and large amounts of money repairing the impact to their credit.¹³

3 68. The danger of identity theft is compounded when a minor's Personal and
4 Medical Information is compromised because minors typically have no credit reports
5 to monitor. Thus, it can be difficult to monitor because a minor cannot simply place
6 an alert on their credit report or "freeze" their credit report when no credit report
7 exists.

8 69. Defendant did not even offer free identity monitoring to Plaintiff and the
9 Class. And even if it did, offering such for a limited period of time would still be
10 insufficient. While some harm has begun already, the worst may be yet to come. There
11 may be a time lag between when harm occurs versus when it is discovered, and also
12 between when Personal and Medical Information is stolen and when it is used. In any
13 case, identity monitoring only alerts someone to the fact that they have already been
14 the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's
15 Personal and Medical Information)—it does not prevent identity theft.¹⁴ This is
16 especially true for many kinds of medical identity theft, for which most credit
17 monitoring plans provide little or no monitoring or protection.

18 70. As a direct and proximate result of the Data Breach, Plaintiff and the
19 Class have been placed at an imminent, immediate, and continuing increased risk of
20 harm from fraud and identity theft. Plaintiff and the Class must now take the time
21 and effort to mitigate the actual and potential impact of the Data Breach on their
22 everyday lives, including placing "freezes" and "alerts" with credit reporting
23 agencies, contacting their financial institutions, healthcare providers, closing or
24 modifying financial accounts, and closely reviewing and monitoring bank accounts,

25
26
27 ¹³ "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013),
<http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf>.

28 ¹⁴ See, *e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017,
<https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html>.

1 credit reports, and health insurance account information for unauthorized activity for
2 years to come.

3 71. Plaintiff and the Class have suffered, and continue to suffer, actual harms
4 for which they are entitled to compensation, including:

5 a. Trespass, damage to, and theft of their personal property including
6 Personal and Medical Information;

7 b. Improper disclosure of their Personal and Medical Information;

8 c. The imminent and certainly impending injury flowing from potential fraud
9 and identity theft posed by their Personal and Medical Information being
10 placed in the hands of criminals and having been already misused;

11 d. The imminent and certainly impending risk of having their confidential
12 medical information used against them by spam callers to defraud them;

13 e. Damages flowing from Defendant's untimely and inadequate notification
14 of the data breach;

15 f. Loss of privacy suffered as a result of the Data Breach, including the harm
16 of knowing cyber criminals have their Personal and Medical Information and
17 that fraudsters have already used that information to initiate spam calls to
18 members of the Class;

19 g. Ascertainable losses in the form of out-of-pocket expenses and the value
20 of their time reasonably expended to remedy or mitigate the effects of the
21 data breach;

22 h. Ascertainable losses in the form of deprivation of the value of
23 customers' personal information for which there is a well-established and
24 quantifiable national and international market;

25 i. The loss of use of and access to their credit, accounts, and/or funds;

26 j. Damage to their credit due to fraudulent use of their Personal and
27 Medical Information; and
28

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

72. Moreover, Plaintiff and the Class have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

73. Despite acknowledging the harm caused by the Data Breach on Plaintiff and Class members, Defendant does nothing to reimburse Plaintiff and Class members for the injuries they have already suffered.

V.

CLASS ACTION ALLEGATIONS

74. Plaintiff brings this action on behalf of himself, the general public, and all other persons similarly situated pursuant to Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure.

75. Class Representative brings this action on his own behalf and on behalf of all other persons similarly situated. The putative class that Class Representative seeks to represent is composed of:

All citizens of the State of California who were patients of Lincare Inc. on or before September 10, 2021, and who received notices from Lincare that their information was compromised (hereinafter the “Class”).

Excluded from the Class are the natural persons who are directors, and officers, of the Defendant. Class Representative expressly disclaims that he is seeking a class-wide recovery for personal injuries attributable to Defendant’s conduct.

76. This action has been brought and may be properly maintained as a class action, pursuant to the Federal Rule of Civil Procedure 23.

77. Numerosity: Although Plaintiff does not, as yet, know the exact size of the class defined above, based upon the nature of the Defendants’ business, Plaintiff is informed and believes that there are numerous members of the class defined above, and that such members are geographically dispersed throughout the State of California. Thus, the class defined above is sufficiently numerous to make joinder

1 impracticable. The disposition of the claims of the members of the class defined above
 2 through this class action will benefit both the parties and this Court. In addition, the
 3 class defined above is readily identifiable from information and records in the
 4 possession of Defendants as well as the members of the class.

5 78. Existence and Predominance of Commons Questions of Fact and Law –
 6 There is a well-defined community of interest among the members of the Class
 7 because common questions of law and fact predominate, Class Representative’s
 8 claims are typical of the members of the class, and Class Representative can fairly
 9 and adequately represent the interests of the Class.

10 79. Common questions of law and fact exist as to all members of the Class
 11 and predominate over any questions affecting solely individual members of the Class.
 12 Among the questions of law and fact common to the Class are:

- 13 (a) Whether Defendant failed to adequately safeguard Plaintiff and the
 14 Class’ Personal and Medical Information;
- 15 (b) Whether Defendant failed to protect Plaintiff and the Class’ Personal and
 16 Medical Information;
- 17 (c) Whether Defendant’s email and computer systems and data security
 18 practices used to protect Plaintiff and the Class’ Personal and Medical
 19 Information violated the FTC Act, HIPAA, CMIA, CCRA and/or
 20 Defendant’s other duties;
- 21 (d) Whether Defendant violated the data security statutes and data breach
 22 notification statutes applicable to Plaintiff and the Class;
- 23 (e) Whether Defendant failed to notify Plaintiff and members of the Class
 24 about the Data Breach expeditiously and without unreasonable delay
 25 after the Data Breach was discovered;
- 26 (f) Whether Defendant engaged in unfair, unlawful, or deceptive practices
 27 by failing to safeguard Breach Victims’ Personal and Medical
 28 Information properly and as promised;
- (g) Whether Defendant acted negligently in failing to safeguard Plaintiff and
 the Class’ Personal and Medical Information, including whether its
 conduct constitutes negligence *per se*;
- (h) Whether Defendant entered into implied contracts with Plaintiff and the
 members of the Class that included contract terms requiring Defendant

to protect the confidentiality of Personal and Medical Information and have reasonable security measures;

- (i) Whether Defendant violated the consumer protection statutes, data breach notification statutes, and state medical privacy statutes applicable to Plaintiff and the Class;
- (j) Whether Defendant failed to notify Plaintiff and Breach Victims about the Data Breach as soon as practical and without delay after the Data Breach was discovered;
- (k) Whether Defendant's conduct described herein constitutes a breach of their implied contracts with Plaintiff and the Class;
- (l) Whether Plaintiff and the members of the Class are entitled to damages as a result of Defendant's wrongful conduct;
- (m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and
- (n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class.

Class Representative's claims are typical of those of the other Class members because Class Representative, like every other Class member, was exposed to virtually identical conduct and are entitled to nominal damages of one thousand dollars (\$1,000) per violation pursuant to Civil Code §§ 56.101 and 56.36(b)(1).

80. Typicality: Plaintiff's claims are typical of the claims of the Class since Plaintiff was notified by Defendants, like all other Class Members, that his medical information and personally identifiable information was unlawfully disclosed to threat actors. Furthermore, Plaintiff and all members of the Class sustained injury in fact by losing their right of privacy in medical information.

81. Adequacy: Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class he seeks to represent; he has retained counsel competent and experienced in complex class action litigation; and intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

1 82. Superiority: The class action is superior to other available means for the
2 fair and efficient adjudication of the claims of Plaintiff and members of the Class.
3 Although the monetary injury suffered by each individual Class member may total
4 several hundred dollars, injury of such magnitude is nonetheless relatively small given
5 the burden and expense of individual prosecution of the complex and extensive
6 litigation necessitated by Defendants' conduct. It would be virtually impossible for
7 members of the Class individually to redress effectively the wrongs done to them.
8 Even if the members of the Class could afford such individual litigation, the court
9 system could not. Individualized litigation presents a potential for inconsistent or
10 contradictory judgments. Individualized litigation increases the delay and expense to
11 all parties, and to the court system, presented by the complex legal and factual issues
12 of the case. By contrast, the class action device presents far fewer management
13 difficulties, and provides the benefits of single adjudication, economy of scale, and
14 comprehensive supervision by a single court.

15 83. Proper and sufficient notice of this action may be provided to each class
16 member through notice by such means as direct mail, electronic mail, publication on
17 the internet, and/or television, radio, and/or print media outlets.

18 84. Plaintiff and the Class Members have suffered irreparable harm and
19 damages as a result of Defendants' wrongful conduct as alleged herein, which is
20 ongoing. Absent a representative action, Plaintiff and each Class Member continue to
21 be damaged, thereby allowing these violations of law to proceed without remedy, and
22 allowing Defendants to continue their wrongful conduct. The prosecution of separate
23 actions by individual members of the Class would create a risk of inconsistent or
24 varying adjudications with respect to individual members of the Class, which would
25 establish incompatible standards of conduct for the Defendant in the State of
26 California and would lead to repetitious trials of the numerous common questions of
27 fact and law in the State of California. Class Representative knows of no difficulty
28 that will be encountered in the management of this litigation that would preclude its

1 maintenance as a class action. As a result, a class action is superior to other available
2 methods for the fair and efficient adjudication of this controversy.

3 85. Moreover, the Class members' individual damages are insufficient to
4 justify the cost of litigation, so that in the absence of class treatment, Defendant's
5 violations of law inflicting substantial damages in the aggregate would go unremedied
6 without certification of the Class. Absent certification of this action as a class action,
7 Class Representative will continue to be damaged by the unauthorized release of their
8 individual identifiable medical information.

9 VI.

10 **CLAIMS FOR RELIEF**

11 **FIRST CLAIM FOR RELIEF**

12 **(Violations of the Confidentiality of Medical Information Act, Civil Code § 56,**
13 ***et seq.*)**

14 **(Against All Defendants)**

15 86. Plaintiff and the Class incorporate by reference all of the above
16 paragraphs of this Complaint as though fully stated herein.

17 87. Defendant is a "provider of health care," within the meaning of Civil
18 Code § 56.05(m), and maintained and continues to maintain "medical information,"
19 within the meaning of Civil Code § 56.05(j), of "patients" of the Defendant, within
20 the meaning of Civil Code § 56.05(k).

21 88. Plaintiff and the Class are "patients" of Defendant within the meaning of
22 Civil Code § 56.05(k). Furthermore, Plaintiff and the Class, as patients of Defendant,
23 had their individually identifiable "medical information," within the meaning of Civil
24 Code § 56.05(j), stored onto Defendant's server through their school districts, on or
25 before December 28, 2021.

26 89. On or about September 26, 2021, Defendant determined that the illegally
27 accessed files involved Plaintiff and the Class members' individual identifiable
28

1 “medical information,” within the meaning of Civil Code § 56.05(j),¹⁵ including
 2 Plaintiff and the Class members’ “name, medical information, which may include
 3 information concerning medical treatments you received such as provider name, dates
 4 of service, diagnosis/procedure, and/or account or record numbers.”

5 90. Defendant was made aware of an unusual activity involving certain of
 6 its electronic files. Defendant immediately commenced an investigation to quickly
 7 assess the security of its systems. Through the investigation, Defendant determined
 8 that certain files were accessed and acquired between September 10, 2021 and
 9 September 29, 2021 without authorization. During its investigation, Defendant
 10 determined that the information of certain individuals were present in the relevant
 11 files.

12 91. As a result of Defendant’s above-described conduct, Plaintiff and the
 13 Class have suffered damages from the unauthorized release of their individual
 14 identifiable “medical information” made unlawful by Civil Code §§ 56.10 and 56.101.

15 92. Because Civil Code § 56.101 allows for the remedies and penalties
 16 provided under Civil Code § 56.36(b), Plaintiff, individually and on behalf of the
 17 Class, seek nominal damages of one thousand dollars (\$1,000) for each violation
 18 under Civil Code § 56.36(b)(1); and Plaintiff individually seeks actual damages
 19 suffered, if any, pursuant to Civil Code § 56.36(b)(2).

20 //

21 //

22 //

23 //

24 ¹⁵ Pursuant to Civil Code § 56.05(j), “Medical information” means “any individually identifiable information, in
 25 electronic or physical form, in possession of or derived from a provider of health care...regarding a patient’s medical
 26 history, mental or physical condition, or treatment. ‘Individually Identifiable’ means that the medical information
 27 includes or contains any elements of personal identifying information sufficient to allow identification of the
 28 individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number,
 or other information that, alone or in combination with other publicly available information, reveals the individual’s
 identity.” As alleged herein, Defendant’s unencrypted server contained Plaintiff’s and the Class members’ names,
 dates of birth, and prescription information, and thus contained individually identifiable medical information as
 defined by Civil Code § 56.05(j)

SECOND CLAIM FOR RELIEF
(Violations of the CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §17200, *et seq.*)

93. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

94. Defendant does business in California. Defendant violated California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

- a. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard their Personal and Medical Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that they did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Class' Personal and Medical Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class' Personal and Medical Information;
- b. by soliciting and collecting Class members' Personal and Medical Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class members' Personal and Medical Information in an unsecure electronic environment;
- c. by failing to disclose the Data Breach in a timely and accurate manner, in violation of Cal. Civ. Code §1798.82;

- d. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq.*;
- e. by violating the CMIA, Cal. Civ. Code § 56, *et seq.*; and
- f. by violating the CCRA, Cal. Civ. Code § 1798.82.

95. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, CMIA, Cal. Civ. Code § 56, *et seq.*, and the CCRA, Cal. Civ. Code § 1798.81.5.

96. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their Personal and Medical Information, and additional losses described above.

97. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Class members' Personal and Medical Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

98. The conduct and practices described above emanated from California where decisions related to Defendant's advertising and data security were made.

99. Plaintiff seeks relief under the UCL, including restitution to the Class of money or property that the Defendant may have acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief,

1 attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and
 2 injunctive or other equitable relief.

3
 4 **THIRD CLAIM FOR RELIEF**
 5 **(Violations of the CALIFORNIA CONSUMER RECORDS ACT, Cal. Civ.**
 6 **Code § 1798.82, et seq.)**

7 100. Plaintiff incorporates by reference all allegations of the preceding
 8 paragraphs as though fully set forth herein.

9 101. Section 1798.2 of the California Civil Code requires any “person or
 10 business that conducts business in California, and that owns or licenses
 11 computerized data that includes personal information” to “disclose any breach of the
 12 security of the system following discovery or notification of the breach in the security
 13 of the data to any resident of California whose unencrypted personal information was,
 14 or is reasonably believed to have been, acquired by an unauthorized person.”
 15 Under section 1798.82, the disclosure “shall be made in the most expedient time
 16 possible and without unreasonable delay”

17 102. The CCRA further provides: “Any person or business that maintains
 18 computerized data that includes personal information that the person or business does
 19 not own shall notify the owner or licensee of the information of any breach of the
 20 security of the data immediately following discovery, if the personal information was,
 21 or is reasonably believed to have been, acquired by an unauthorized person.” Cal. Civ.
 22 Code § 1798.82(b).

23 103. Any person or business that is required to issue a security breach
 24 notification under the CCRA shall meet all of the following requirements:

- 25 a. The security breach notification shall be written in plain language;
- 26 b. The security breach notification shall include, at a minimum, the
 27 following information:
 - 28 i. The name and contact information of the reporting person or
 business subject to this section;

- ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
- iii. If the information is possible to determine at the time the notice is provided, then any of the following:
 - 1. The date of the breach;
 - 2. The estimated date of the breach; or
 - 3. The date range within which the breach occurred. The notification shall also include the date of the notice.
- iv. Whether notification was delayed as a result of law enforcement investigation, if that information is possible to determine at the time the notice is provided;
- v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
- vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

104. The Data Breach described herein constituted a "breach of the security system" of Defendant.

105. As alleged above, Defendant unreasonably delayed informing Plaintiff and Class members about the Data Breach, affecting their Personal and Medical Information, after Defendant knew the Data Breach had occurred.

106. Defendant failed to disclose to Plaintiff and the Class, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal and Medical Information when Defendant knew or reasonably believed such information had been compromised.

107. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

1 108. Upon information and belief, no law enforcement agency instructed
2 Defendant that timely notification to Plaintiff and the Class would impede its
3 investigation.

4 109. As a result of Defendant's violation of Cal. Civ. Code § 1798.82,
5 Plaintiff and the Class were deprived of prompt notice of the Data Breach and were
6 thus prevented from taking appropriate protective measures, such as securing identity
7 theft protection or requesting a credit freeze. These measures could have prevented
8 some of the damages suffered by Plaintiff and Class members because their stolen
9 information would have had less value to identity thieves.

10 110. As a result of Defendant's violation of Cal. Civ. Code § 1798.82,
11 Plaintiff and the Class suffered incrementally increased damages separate and distinct
12 from those simply caused by the Data Breach itself.

13 111. Plaintiff and the Class seek all remedies available under Cal. Civ. Code
14 § 1798.84, including, but not limited to the damages suffered by Plaintiff and the other
15 Class members as alleged above and equitable relief.

16 112. Defendant's misconduct as alleged herein is fraud under Cal. Civ. Code
17 § 3294(c)(3) in that it was deceit or concealment of a material fact known to the
18 Defendant conducted with the intent on the part of Defendant of depriving Plaintiff
19 and the Class of "legal rights or otherwise causing injury." In addition, Defendant's
20 misconduct as alleged herein is malice or oppression under Cal. Civ. Code §
21 3294(c)(1) and (c) in that it was despicable conduct carried on by Defendant with a
22 willful and conscious disregard of the rights or safety of Plaintiff and the Class and
23 despicable conduct that has subjected Plaintiff and the Class to cruel and unjust
24 hardship in conscious disregard of their rights. As a result, Plaintiff and the Class are
25 entitled to punitive damages against Defendant under Cal. Civ. Code § 3294(a).

26 //

27 //

28 //

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the Court to grant Plaintiff and the Class members the following relief against Defendant:

a. An order certifying this action as a class action under Code of Civil Procedure §382, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, including statutory damages under the CMIA, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein, including, but not limited to:

- i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- iii. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
- iv. Ordering that Defendant's segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

- 1 v. Ordering that Defendant purge, delete, and destroy in a reasonably
 2 secure manner customer data not necessary for its provisions of
 3 services;
 4 vi. Ordering that Defendant conduct regular database scanning and
 5 securing checks;
 6 vii. Ordering that Defendant routinely and continually conduct
 7 internal training and education to inform internal security
 8 personnel how to identify and contain a breach when it occurs and
 9 what to do in response to a breach; and
 10 viii. Ordering Defendant to meaningfully educate its current, former,
 11 and prospective employees and subcontractors about the threats
 12 they face as a result of the loss of their financial and personal
 13 information to third parties, as well as the steps they must take to
 14 protect themselves.;
- 15 d. An order requiring Defendant to pay the costs involved in notifying the
 16 Class members about the judgment and administering the claims process;
- 17 e. A judgment in favor of Plaintiff and the Class awarding them pre-
 18 judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses
 19 as allowable by law, including the CCRA, Cal. Civ. Code § 1798.84(g), UCL, Cal.
 20 Bus. & Prof. Code § 17082, CMIA, Cal. Civ. Code 56.35; and
- 21 f. An award of such other and further relief as this Court may deem just
 22 and proper.

23 **POTTER HANDY LLP**

24 /s/ James M. Treglio

25 Dated: August 29, 2022

By:

26 _____
 27 Mark D. Potter, Esq.

James M. Treglio, Esq.

28 Attorneys for the Plaintiff and the Class

DEMAND FOR JURY TRIAL

Plaintiff and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

POTTER HANDY LLP

/s/ James M. Treglio

Dated: August 29, 2022

By:

Mark D. Potter, Esq.
James M. Treglio, Esq.
Attorneys for the Plaintiff and the Class

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that, on August 29, 2022, a true and correct copy of the FIRST AMENDED CLASS ACTION COMPLAINT was filed electronically. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system and indicated on the Notice of Electronic Filing. Parties may access this filing through the Court's EM/ECF System.

James Treglio

James M. Treglio, Esq.